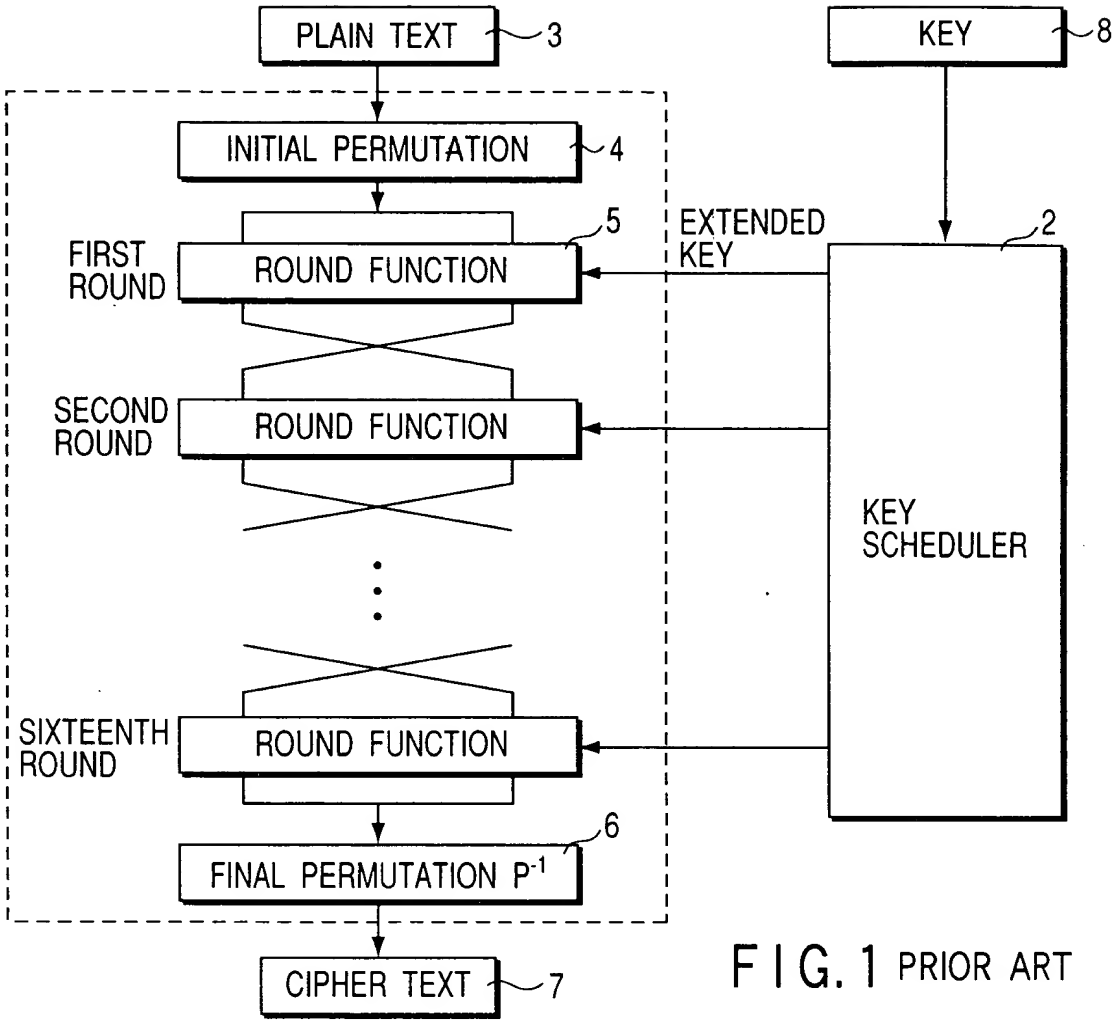



FIG. 1 PRIOR ART

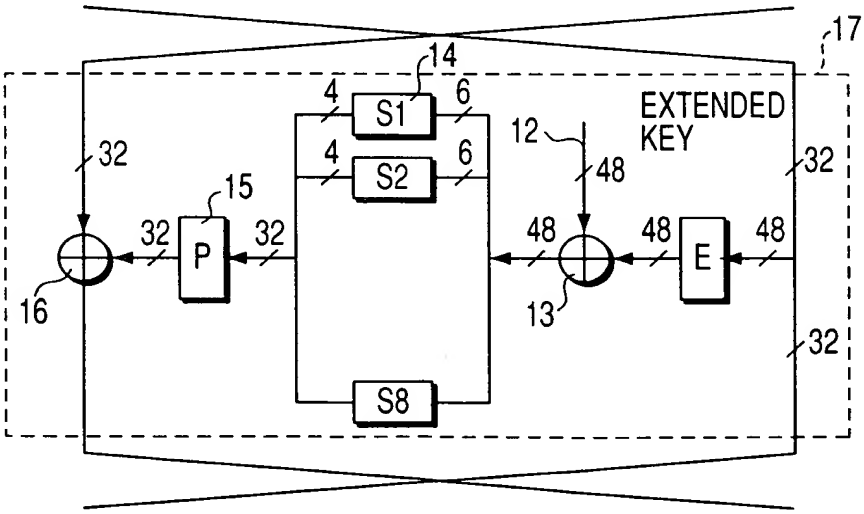



FIG. 2
PRIOR ART

TABLE OF S1

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14, | 4, | 13, | 1, | 2, | 15, | 11, | 8, | 3, | 10, | 6, | 12, | 5, | 9, | 0, | 7, |
| 0, | 15, | 7, | 4, | 14, | 2, | 13, | 1, | 10, | 6, | 12, | 11, | 9, | 5, | 3, | 8, |
| 4, | 1, | 14, | 8, | 13, | 6, | 2, | 11, | 15, | 12, | 9, | 7, | 3, | 10, | 5, | 0, |
| 15, | 12, | 8, | 2, | 4, | 9, | 1, | 7, | 5, | 11, | 3, | 14, | 10, | 0, | 6, | 13, |

FIG. 3

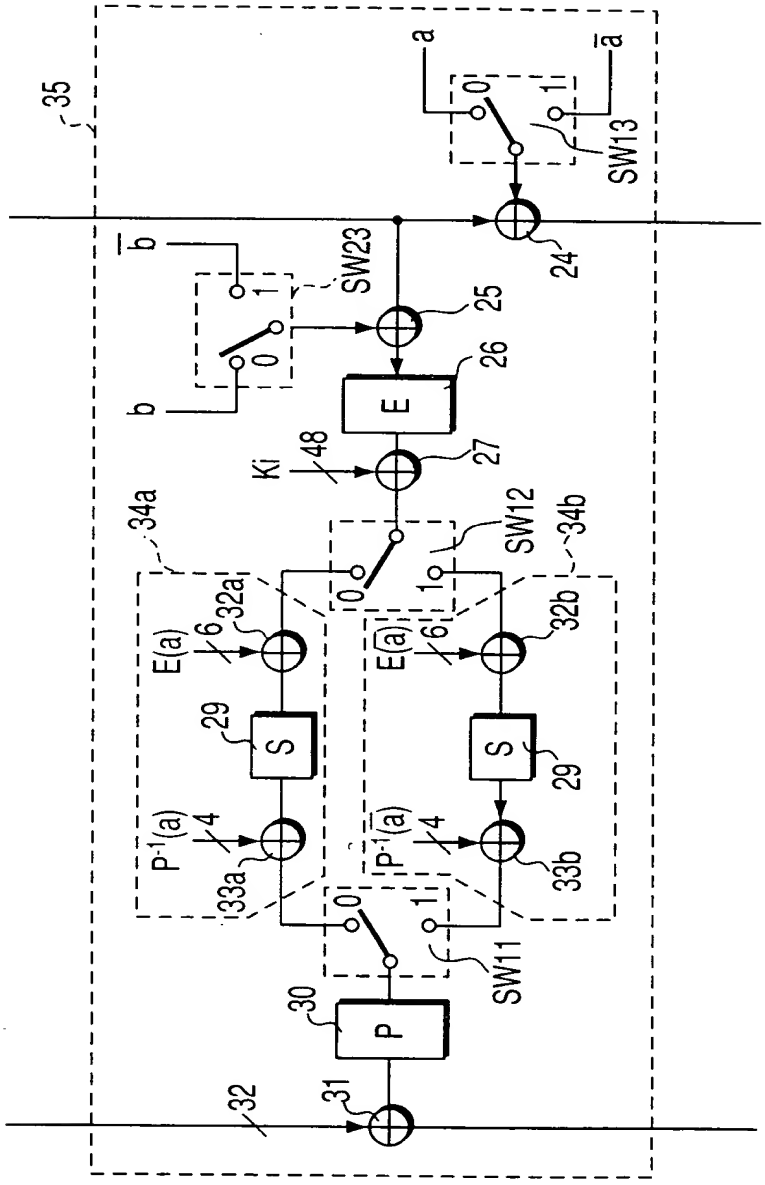



FIG. 4

FIG. 5A

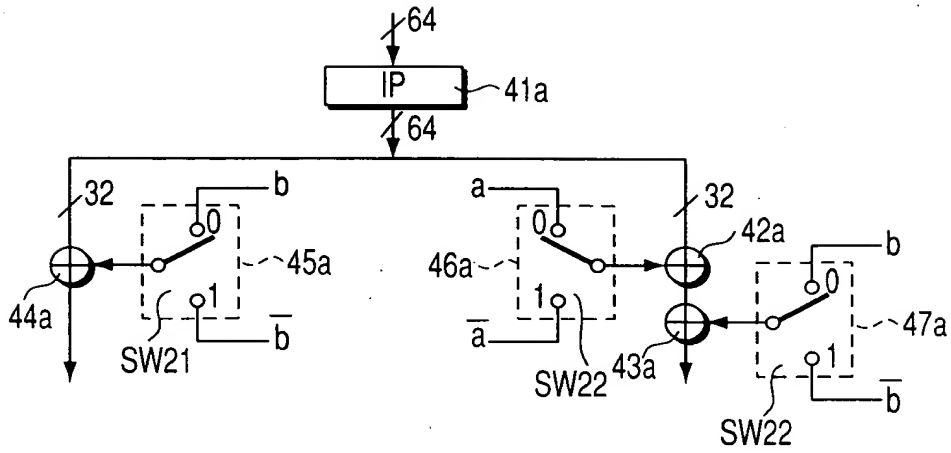



FIG. 5B

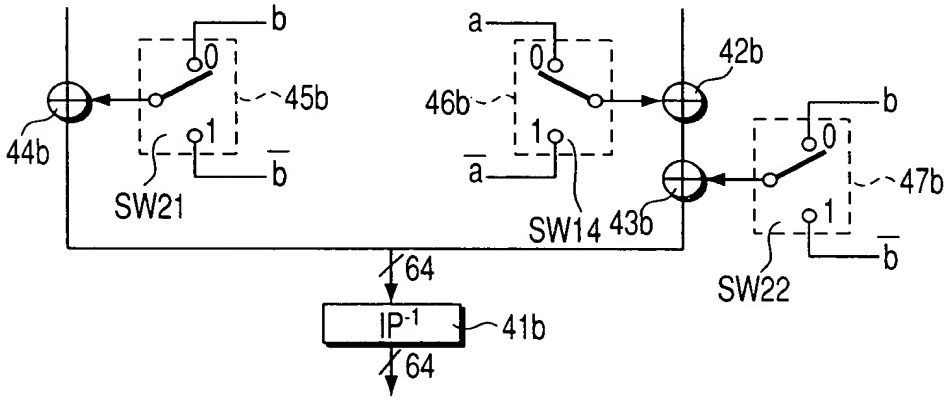



FIG. 6

TABLE OF EXPANSION E

| | | | | | |
|---|---|---|---|---|---|
| 32, | 1, | 2, | 3, | 4, | 5, |
| 4, | 5, | 6, | 7, | 8, | 9, |
| 8, | 9, | 10, | 11, | 12, | 13, |
| 12, | 13, | 14, | 15, | 16, | 17, |
| 16, | 17, | 18, | 19, | 20, | 21, |
| 20, | 21, | 22, | 23, | 24, | 25, |
| 24, | 25, | 26, | 27, | 28, | 29, |
| 28, | 29, | 30, | 31, | 32, | 1, |

FIG. 7

TABLE OF PERMUTATION P

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 16, | 7, | 20, | 21, | 29, | 12, | 28, | 17, | 1, | 15, | 23, | 26, | 5, | 18, | 31, | 10, |
| 2, | 8, | 24, | 14, | 32, | 27, | 3, | 9, | 19, | 13, | 30, | 6, | 22, | 11, | 4, | 25, |

OUTPUT OF CONCEALED S1 WHEN INPUT CORRESPONDS TO (000000, 000001,···,111111) IN CASE OF MASK a

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | 11 | 14 | 2 | 13 | 4 | 0 | 15 | 1 | 7 | 11 | 1 | 6 | 13 | 5 | 8 | 15 | 12 | 4 | 9 | 3 | 10 | 9 | | |
| 3 | 10 | 0 | 7 | 14 | 12 | 6 | 2 | 5 | 4 | 2 | 8 | 1 | 7 | 11 | 11 | 16 | 14 | 4 | 13 | 8 | 9 | 7 | 6 | |
| 13 | 10 | 9 | 1 | 14 | 0 | 12 | 12 | 0 | 5 | 15 | 2 | 5 | 3 | 10 | 15 | 3 | | | | | | | | |

FIG. 8

TABLE OF MASK $\bar{a}$ (BIT INVERSION OF a)

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 | 0 | 5 | 12 | 10 | 13 | 0 | 10 | 15 | 3 | 3 | 15 | 1 | 14 | 6 | 5 | 2 | 9 | 8 | 6 | 7 | 2 | 11 | 1 | 9 |
| 4 | 4 | 8 | 14 | 7 | 13 | 11 | 10 | 1 | 3 | 9 | 3 | 1 | 8 | 15 | 5 | 12 | 6 | 5 | 12 | 6 | 11 | 3 | 0 | 7 |
| 10 | 2 | 9 | 14 | 4 | 8 | 14 | 0 | 15 | 11 | 2 | 13 | 1 | 4 | 7 | | | | | | | | | | |

FIG. 9



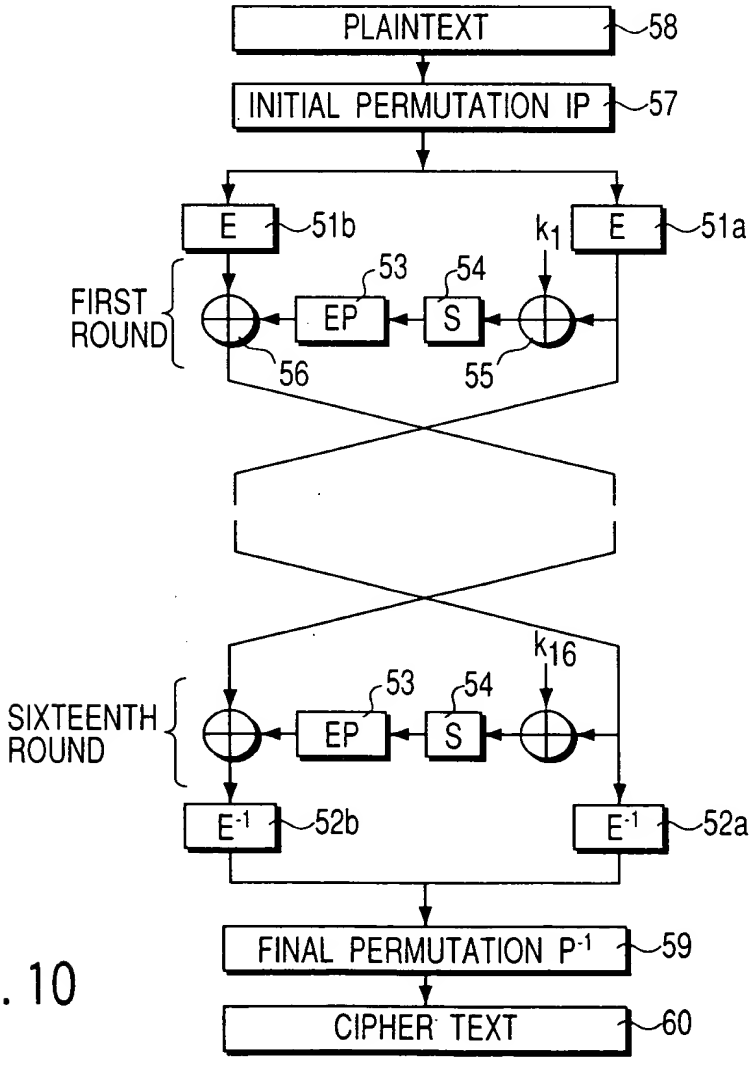



FIG. 10

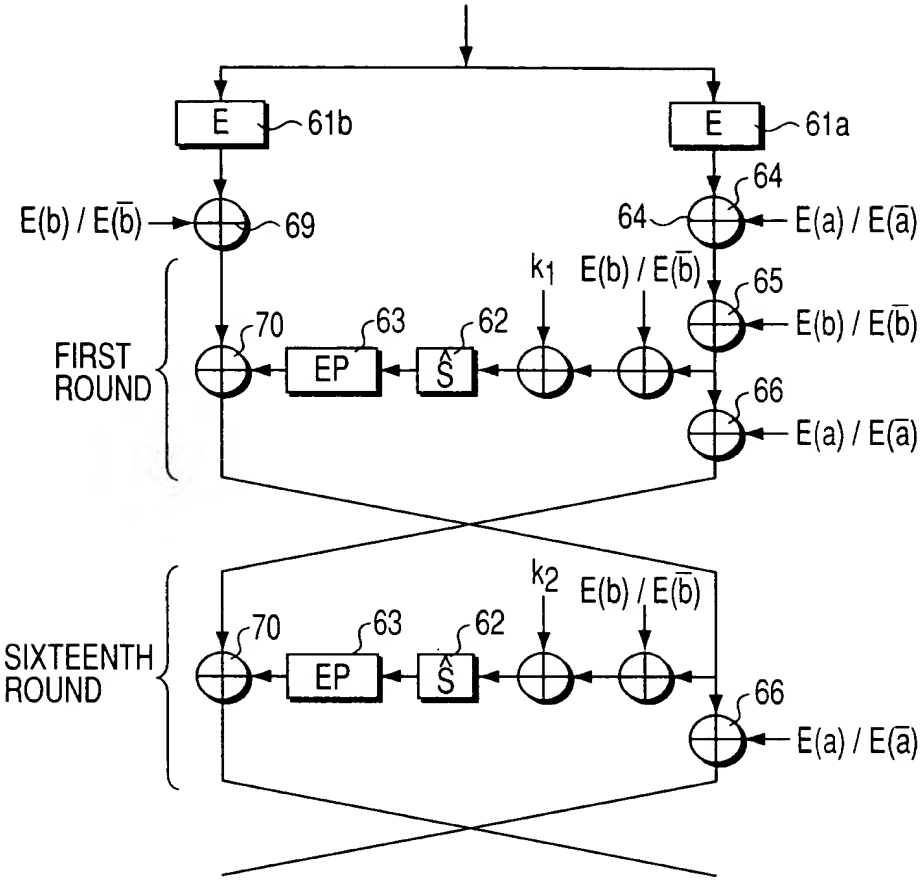



FIG. 11

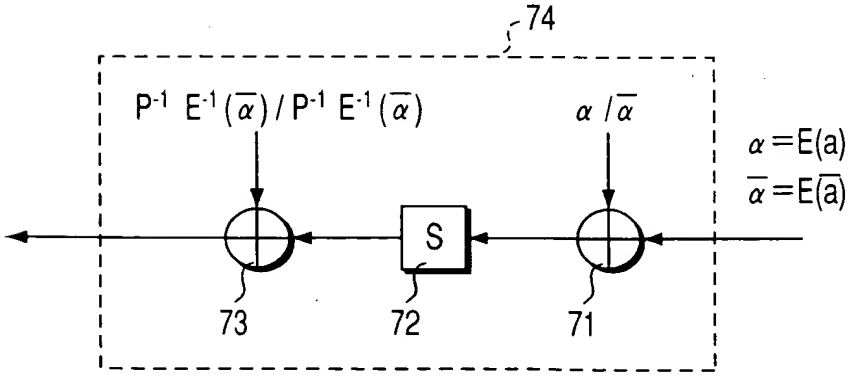



FIG. 12

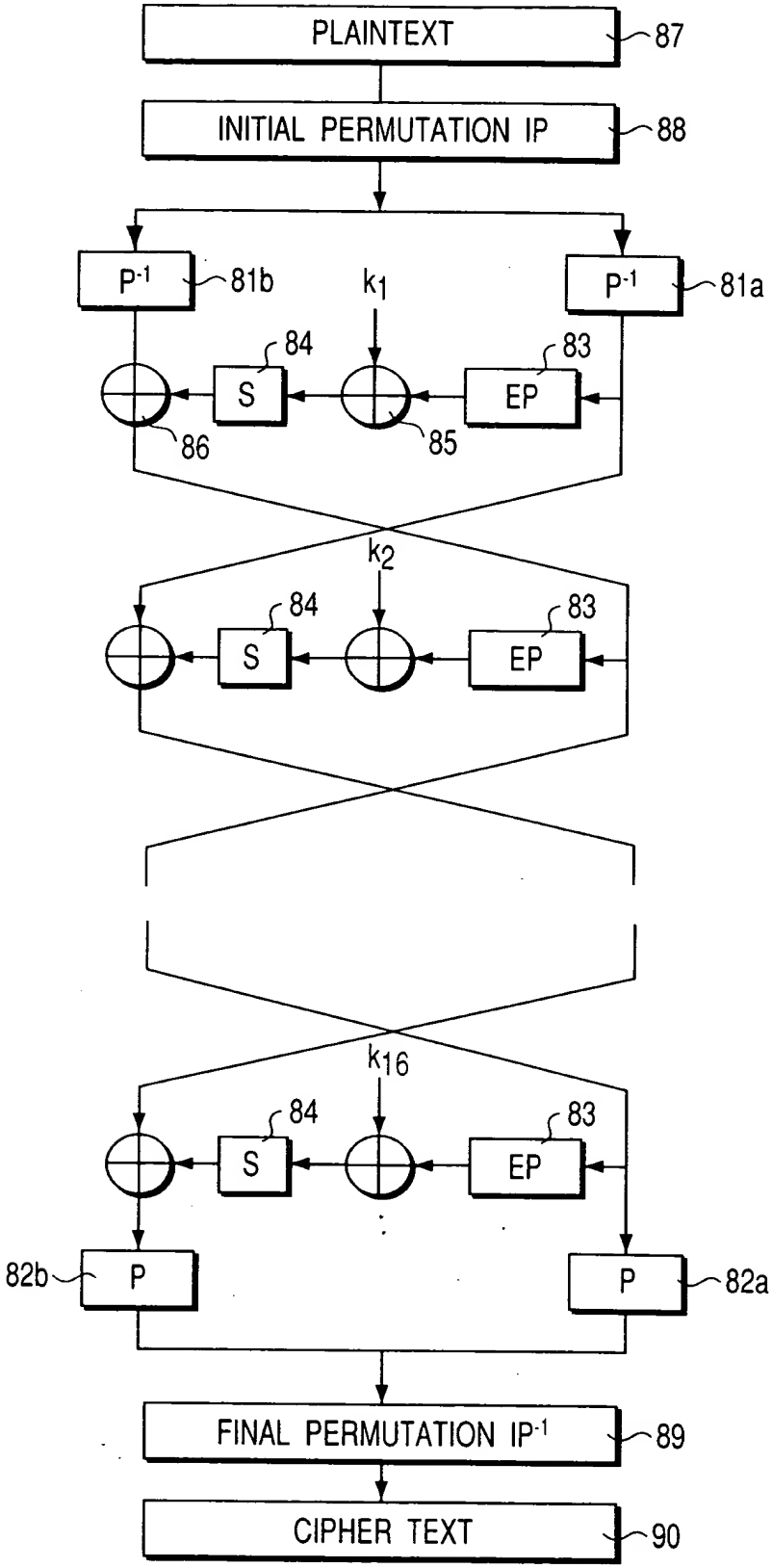



FIG. 13

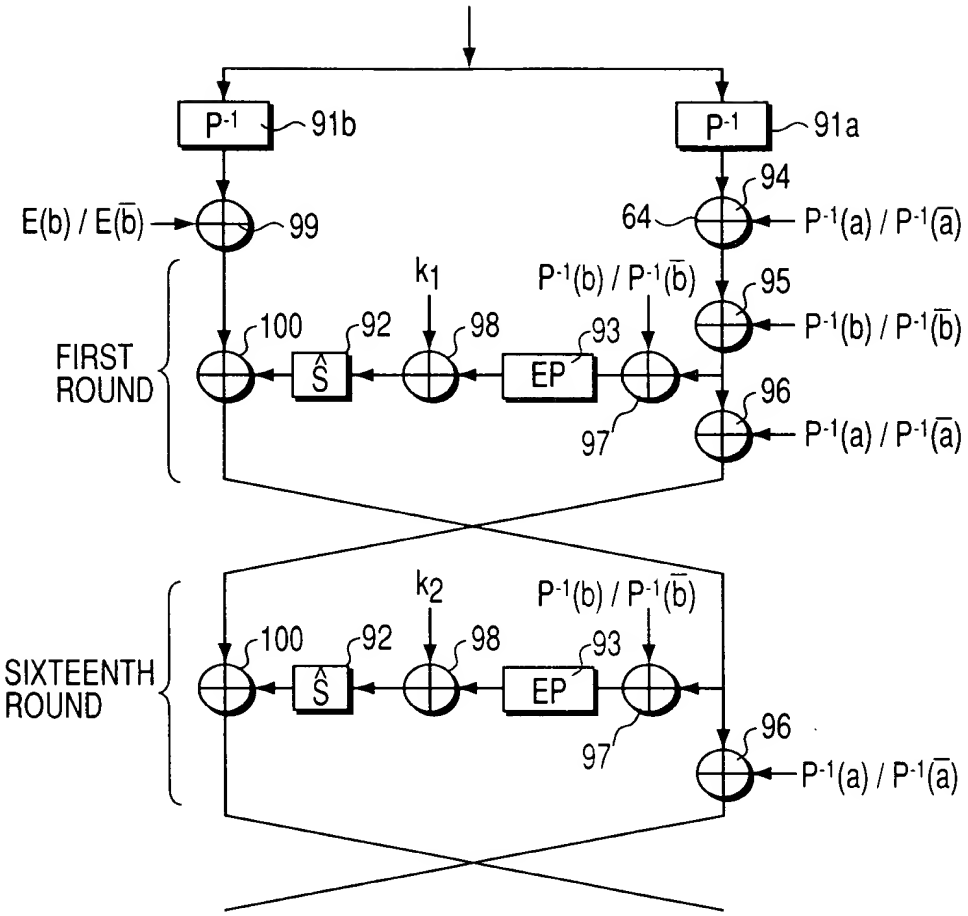



FIG. 14

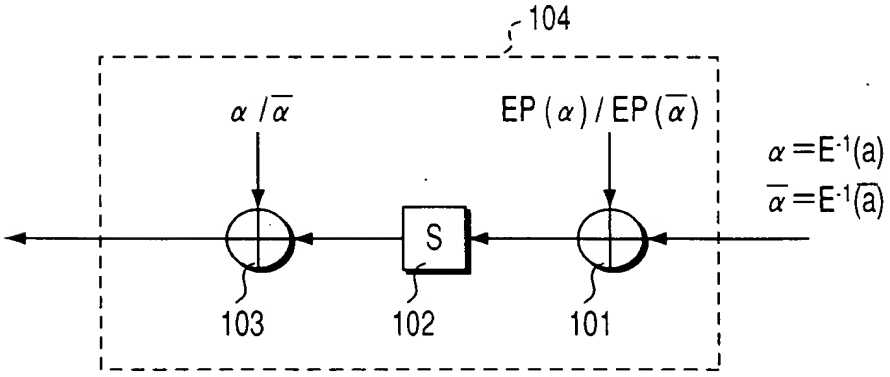



FIG. 15

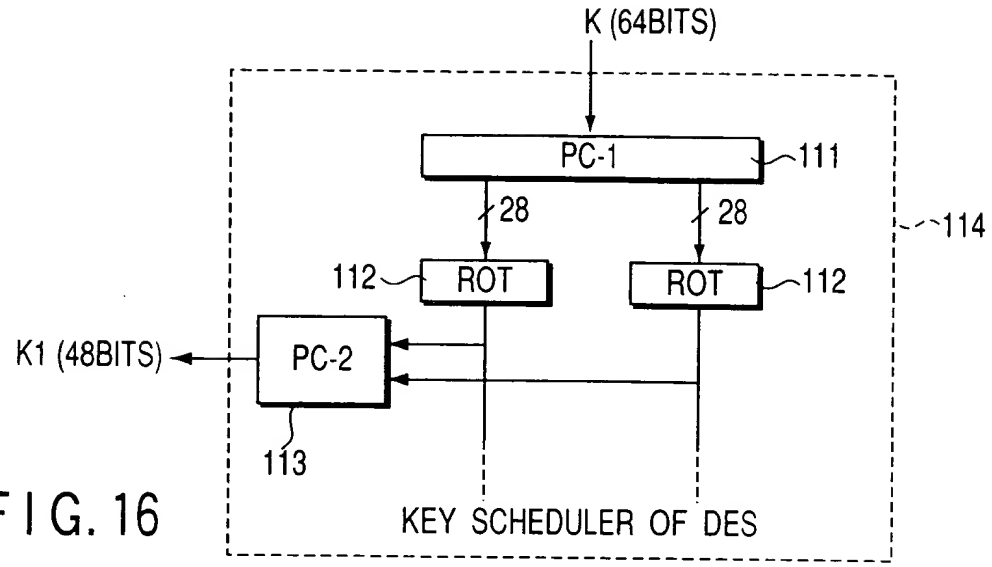



FIG. 16

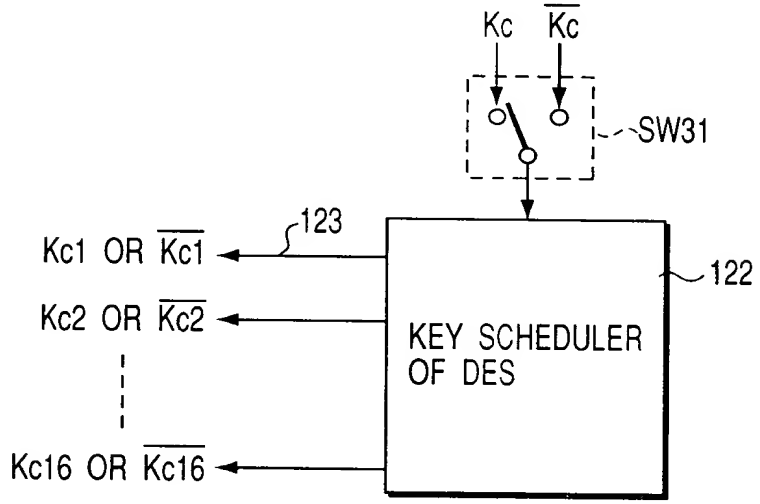



FIG. 17

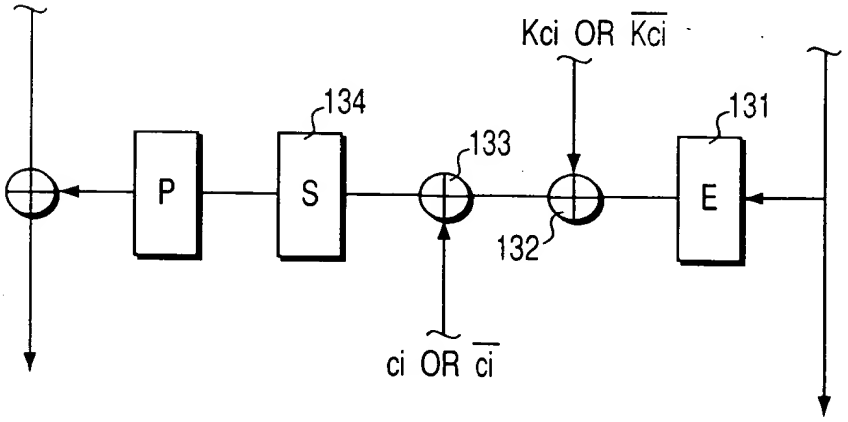



FIG. 18

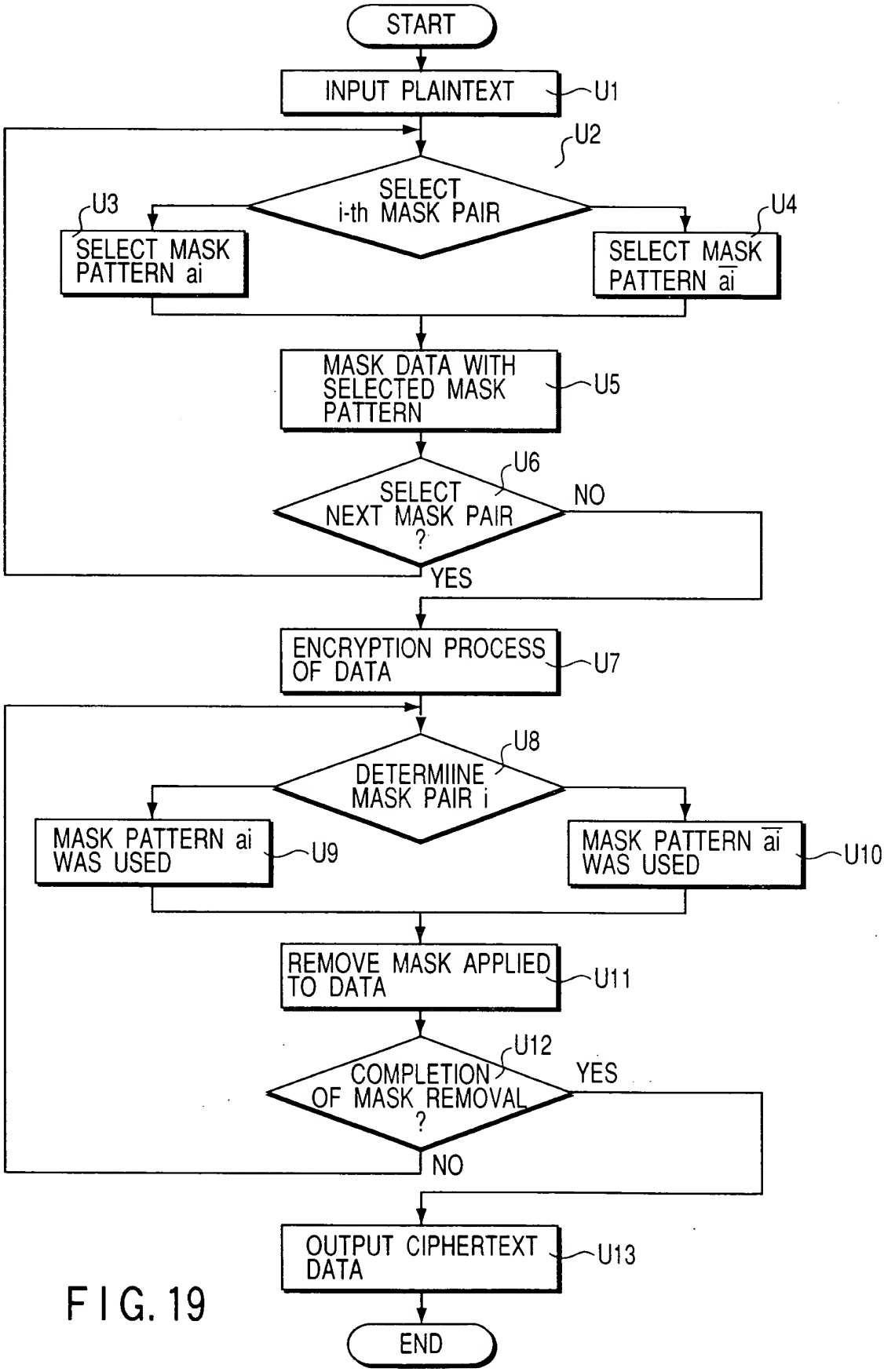



FIG. 19

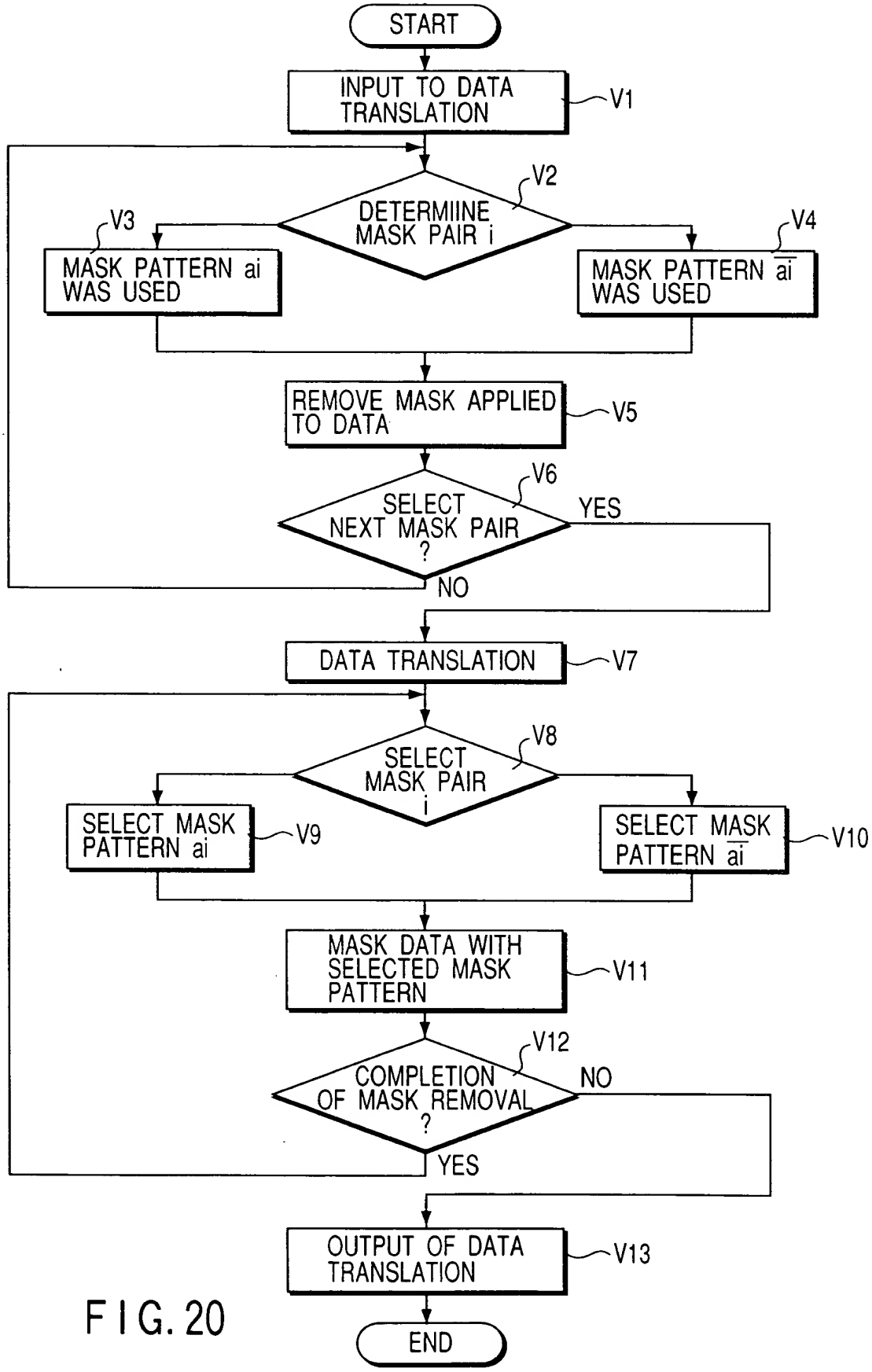



FIG. 20

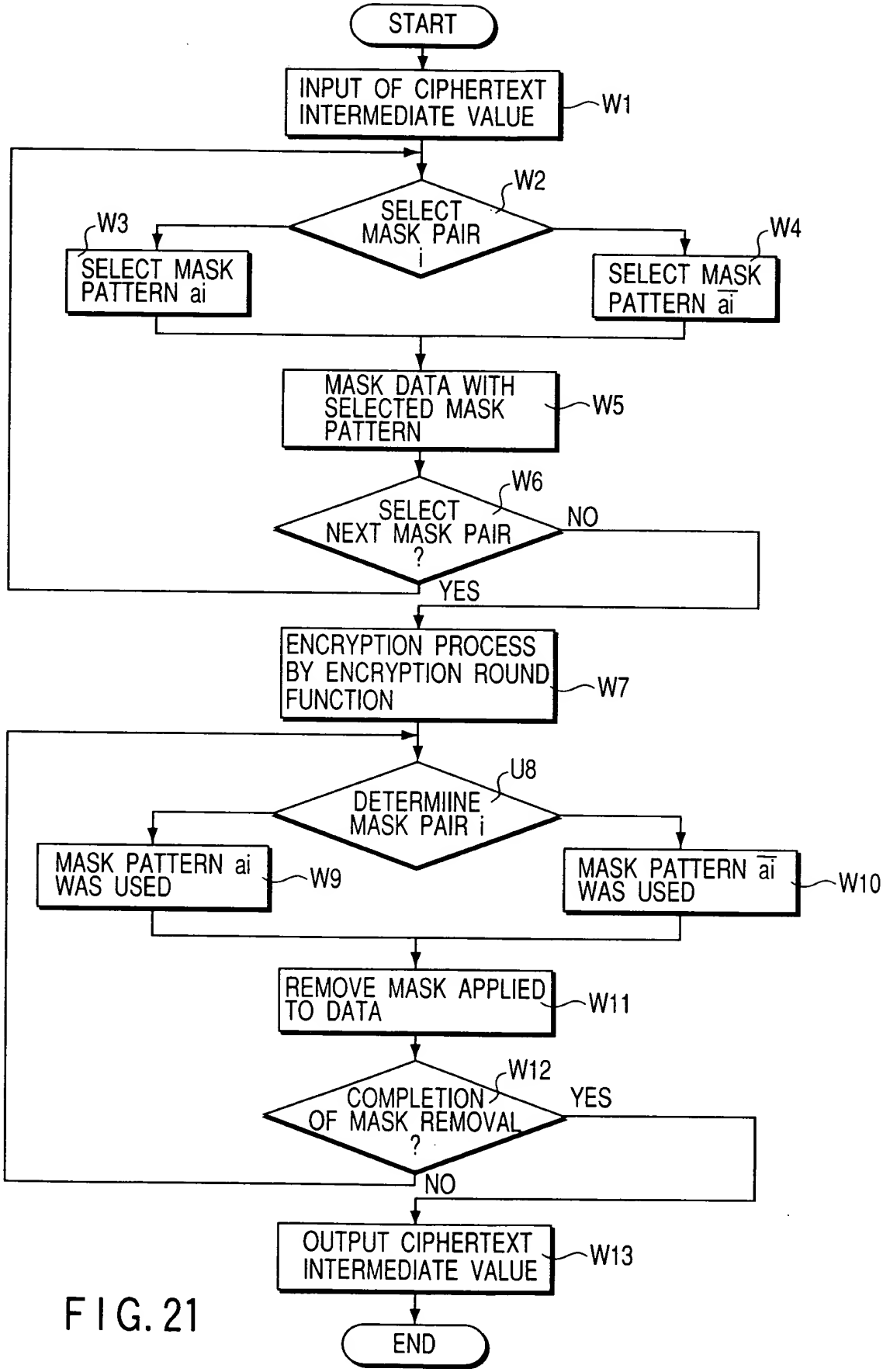
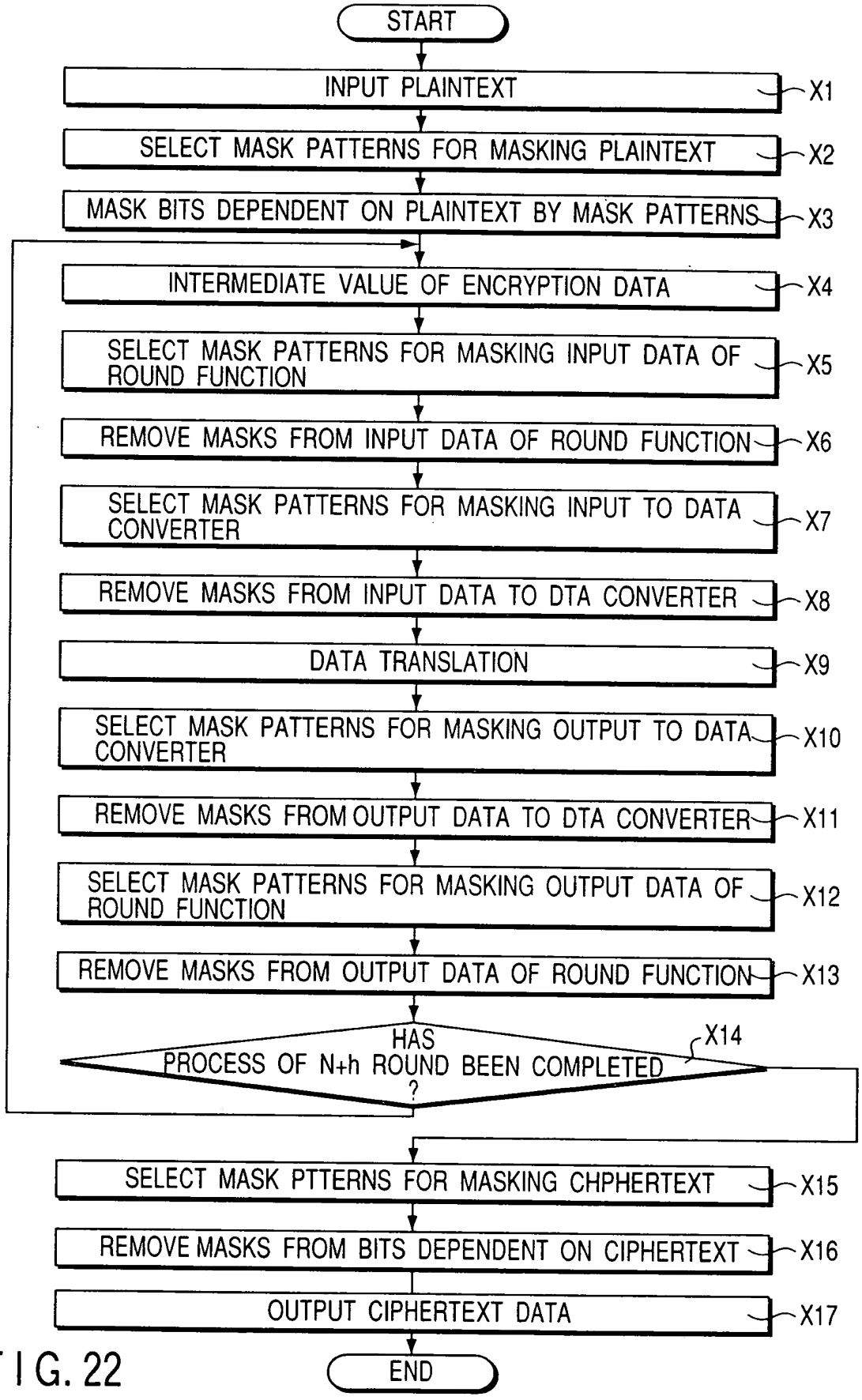



FIG. 21




F I G. 22

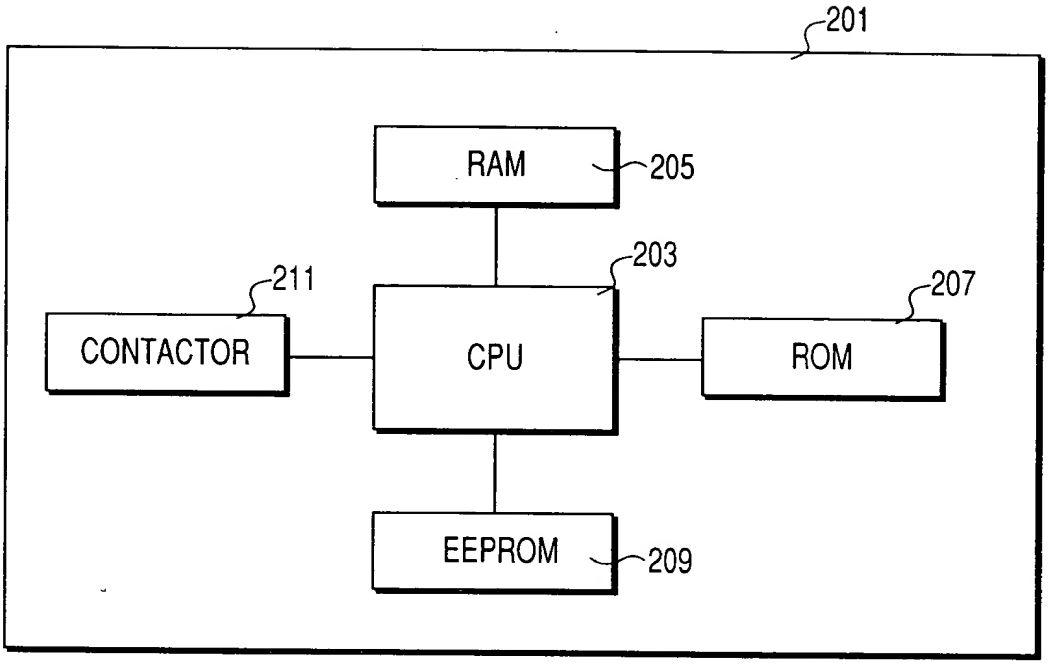



FIG. 23